Spring 05
Ninth Edition

SPRING

Personnel & Document Security Newsletter

USDA/DA/OPPM/PDSD
(202) 720-7373

Special projects in our office:

- e-QIP
- SETS Modernization
- Web Presence

Individual Highlights:

eClearance Initiatives in PDSD: e-QIP Update

Since successfully transmitting our first e-QIP questionnaire to the Office of Personnel Management (OPM) in July 2004, the Personnel and Document Security Division (PDSD) has continually progressed toward our stated goal of 100% implementation of the e-QIP system for all requests for security clearances, using the SF-86, by September 30, 2005. OPM hopes to have the Standard Form 85P available and online by late Spring 2005.

From June 2004 to December 2004, the PDSD coordinated with the OPM to provide e-QIP training for each USDA agency and ensured each agency had at least one personnel security point-of-contact (POC) trained and capable of transmitting forms electronically. Beginning January 3, 2005, the PDSD asked each agency's personnel security POC to submit 25% of all requests for security clearances via the e-QIP system by the end of the second quarter of FY05. Agencies that exceeded or nearly met the 25% goal within the second quarter include the Office of the Inspector General (77%), the Agricultural Research Service (20%), and the Foreign Agricultural Service (22%). The Office of the Chief Information Officer has used the system steadily since gaining access to the system in July 2004 and the Food Safety and Inspection Service closed out the second quarter by initiating 15 new investigations in e-QIP. Unfortunately, usage remains extremely low in other USDA agencies.

Our usage goal will increase to 75% by the end of the third quarter of FY 05, (June 30, 2005) and to 100% by September 30, 2005. After September 30, 2005, the PDSD will no longer accept requests for national security clearances that are not submitted via e-QIP without a written waiver. The PDSD will continue reporting each agency's progress of meeting the quarterly goal for e-QIP submissions, as well as providing progress reports to the USDA's e-Government team for this important Presidential e-Government initiative.

The PDSD has created an instructional e-QIP manual to provide a pictorial step-by-step guide to assist POC's on initiating, reviewing, and approving applicants in the e-QIP system. This guide can be obtained by calling (202) 720-7373.

The PDSD would like to thank all POC's for their hard work in the successful implementation of e-QIP within the USDA. We look forward to working with you in the future as we strive to achieve our ultimate goal of 100% submission for national security forms by September 30, 2005.

SETS Modernization Project

PDSD management visited the National Finance Center (NFC) during the week of March 7th to participate in meetings concerning the modernization of the Secure Entry Tracking System (SETS).

The modernization project will create a web-based SETS system and will be visually similar to USDA's Employee Personal Page. The new, web-based system will allow Agency Personnel Security POC's to have direct, read-only access to information currently contained in PDSD's Personnel Security Database (PSD).

The modernized SETS will eliminate the need for PDSD to operate two databases of personnel security information and will facilitate easier access to information than the current SETS system.

It is undetermined whether the new, modernized system will retain the same name; however, the system is scheduled to be in use by the PDSD no later than fall 2005.

Web Presence update: The new PDSD website

All USDA web sites are currently in the development stages of the Web Presence initiative. The purpose of Web Presence is to enhance each web site's presentation, usability, and overall customer experience. This new look is already visible on the main USDA and the Departmental Administration (DA) home pages.

The new PDSD web site will offer all of our customers a more streamlined connection to forms, security information, and online security training.

The **Automated Briefing System** (ABS), developed by the Defense Personnel Security Research Center, will be part of our enhanced web site. ABS will automate security and threat awareness briefings for personnel with access to classified or other sensitive national security information.

The implementation of the new site is currently underway with the DA Webmaster. We expect final approval from USDA and the eGOV team within the next two months.

Security Tidbits for Holding a Classified Meeting

- Always verify an individual's security clearance and "need-to-know" prior to giving them access to classified information.
- Always check the identification of individuals you do not personally recognize.
- Because most meeting discussions will not entirely involve classified information, always announce when you begin discussing classified information and the classification level you are disclosing. Example: "The following information is classified as SECRET…"
- Always make arrangements to mail notes and handouts to individuals who cannot hand-carry classified information back to their offices.
- Always ensure individuals have the proper storage capabilities for the level of classified documents you wish to give them.
- Always ensure a contract covers the subject matter you plan to share with a contractor.
- When hosting a meeting with non-USDA cleared personnel, you must ensure their security office submits the proper visit authorization to PDSD prior to the classified meeting.

Definition: Suitability

A person's fitness based on character and reputation, for employment by the Federal Government.

Intelligence Reform Law: Reduction in Processing Times

To the extent practical, the new Intelligence Reform Law will require that each authorized adjudicative agency make a determination on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application for a security clearance by an authorized investigative agency. This 60-day average period shall include— a period of no longer than 40 days to complete the investigative phase of the clearance review; and a period of not longer than 20 days to complete the adjudicative phase of the clearance review.

This plan shall take effect 5 years after the date of the enactment of this Act. During this period, each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-day average period shall include—a period of no longer than 90 days to complete the investigative phase of the clearance review; and a period of not longer than 30 days to complete the adjudicative phase of the clearance review. To read this section in full, click on the following link:

Title III: Security Clearances

Security Challenge Pop Quiz!

Test your knowledge on personnel security and information security issues. Want to learn more? Read our online security guide.

1. The Personnel Security program has ____ adjudicative guidelines for determining eligibility for access to classified information.

2. What is the minimum, initial investigation type required for an employee requiring access to Top Secret information?

3. How many classification categories are there for National Security information?

4. This Executive Order sets the U.S. government policy for classifying national security information that must be protected from unauthorized disclosure.

5. The standards set by this Executive Order directs that access shall be granted only to individuals "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."

6. This level of classified material MAY NOT be sent through the mail under any circumstances.

7. Employees holding a Top Secret clearance must be reinvestigation every __ years.

8. The Acronym for Sensitive Compartmented Information is ___.

9. A ____ is an accredited area, room, or installation where SCI may be stored, used, discussed, and/or processed. It provides formal access controls approved by the Director of Central Intelligence to hold information derived from intelligence sources, methods, or analytical processes.

10. Access to National Security information is not granted until the information security indoctrination briefing is successfully concluded and the subject completes the required _____ nondisclosure form.

Definition:

Security Clearance

A determination by an official with specified authority that an individual is trustworthy to have access to classified information or material within a designated classification category for which he or she has a need-to-know.

Interpol Searches

In the interest of providing our customers with the most complete and comprehensive investigative information available, the U.S. Office of Personnel Management (OPM) is partnering with the International Criminal Police Organization, U.S. National Central Bureau (Interpol - USNCB) to conduct Interpol record checks for investigations requiring overseas coverage.

The USNCB was authorized by Federal statute, and it operates within the guidelines prescribed by the Department of Justice, in conjunction with the Department of Homeland Security. Its mission is to facilitate international law enforcement cooperation as the United States representative with Interpol on behalf of the Attorney General. A full explanation of the USNCB and its functions can be found at www.usdoj.gov/usncb.

Under the terms of our agreement with USNCB, an Interpol search will be conducted when, for six months or more, the subject of an investigation: (1) had a non-military foreign residence; (2) had non-military employment overseas; (3) was engaged in academic activities abroad; or (4) when the subject admits to, or there is developed, criminal activity overseas within the investigative coverage period.

If, as a result of an Interpol check, coverage of issues outside the normal scope of an investigation is required, agencies may obtain the coverage by submitting a request for a Reimbursable Suitability/Security Investigation (RSI). The results will be displayed as an "INPL" item on the Case Closing Transmittal (CCT).

DSS transfer to OPM: Latest News

In an interview with Federal Diary Live, Stephen Benowitz, OPM Associate Director, stated OPM has issued contracts with five firms, in addition to US Investigations Services (USIS), to nearly double the number of contract investigators workforce to handle the current and projected workload.

These companies are Omniplex, MSM, CACI, Kroll, and Sa-Tech.

OPM's goal is to complete all national security investigations within 90 days or less, and have agencies adjudicate them those investigations within 30 days (a requirement in the new Intelligence Bill).

The Truth about e-QIP

Does OPM's e-QIP (Electronic Questionnaires for Investigations Processing) truly make completing the 11-page SF-86, Questionnaire for National Security Positions, easier?

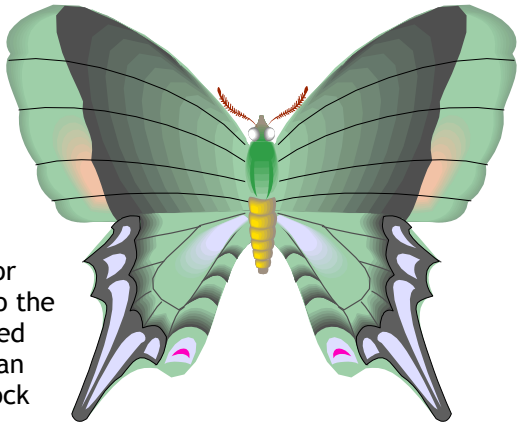
Yes, according to Glenn Haggstrom, Deputy Director, Office of Procurement and Property Management, Departmental Administration. Mr. Haggstrom recently completed his SF-86's from scratch. He has completed SF-86's in both DOD's Electronic Personnel Security Questionnaires (EPSQ) and OPM's e-QIP. He found e-QIP very friendly and, compared with EPSQ, easier to navigate between questions. One advantage of e-QIP is the storage of the data placed in the system. This means the next time he has to update his SF-86, e-QIP will automatically fill-in many of the fields for him, and thus significantly reduce completion time.

When asked what advice he would give to new users of e-QIP, Mr. Haggstrom emphasized that users read the e-QIP instruction's before beginning to complete the form.

CLASSIFIED MATERIAL DESTRUCTION

Guidance on how to properly dispose of classified information can be derived from the Executive Order 12958, as amended, Classified National Security Information, and the implementing directive, Information Security Oversight Office (ISOO) Directive 1.

Basically, all classified material and information must be destroyed in a way that is approved by the National Security Agency (NSA). There are two ways USDA destroys classified information and material.



Pentagon Force Protection Agency Incinerator Plant

The PDSD has made arrangements with the Pentagon Force Protection Agency Incinerator Plant for the destruction of classified paper, plastics, and light metals. They can accept material ranging from unclassified but sensitive to Top Secret – Sensitive Compartmented Information (TS/SCI). They accept documents, CDs, cassettes, VHS tapes, hard drives, and binders. Burn bags can be used for CDs, cassettes, VHS tapes, documents, binders, and viewgraphs. DO NOT PUT GLASS OR METAL IN THE BAGS AND BOXES except clips built into a binder or the metal on CDs, cassettes. Hard drives must have the metal frames removed, placed in a separate box or bag, so we can give those directly to the driver for control. They are delivered to NSA for destruction. Burn bags can be ordered through GSA catalog, stock number 8105-00-262-7363. All bags must be labeled on the outside with the highest level of classified material placed therein, your office name, room number, and telephone number. The bags cannot weight more than 10 pounds and must be stapled shut. Call PDSD to arrange for pick-up at (202) 720-7373.

High Security Cross-cut Shredder

Classified documents and viewgraphs can be destroyed in administrative offices. NSA publishes approved equipment specifications for all devices used to destroy classified information. Their list includes paper shredders, devices used to destroy CD's, diskettes, etc.

Several times a year NSA puts out an Evaluated Products List (EPL). The EPL identifies all machines that have been tested and approved by NSA to destroy national security classified information in accordance with the standards issued by the Executive Order.

The link to the current EPL is: http://www.nsa.gov/ia/government/MDG/EPL_02-01-L_Jan_2005.pdf

If proper procedures are followed, **USDA Field Offices** can mail up to Secret information to the PDSD office for destruction. Higher levels of classified information and equipment requiring destruction should be coordinated with PDSD. For additional guidance, please call PDSD at (202) 720-7373.

Definition:

Security Incident

Any incident involving classified information in which there is a deviation from the requirements of governing security regulations. Examples are compromise, inadvertent disclosure, and need-to-know violation.

Agency Points-of-Contact: Requesting Info from PSB

The Personnel Security Branch (PSB) staff receives numerous requests, via email or telephone, from various agency security points-of-contact requesting status checks, personnel security guidance, documentation, etc.

Requests for lengthy lists of case status checks, guidance/policy information, and such, should be directed to Susan Gulbranson, Chief of Personnel Security, for assignment to PSB staff members.

Unless you are working with a specialist on a particular issue, please do not enlist their assistance without management's approval.

Our Address
1400 Independence Ave, SW
STOP 9305, RMS310
Washington, DC 20250

Phone:
(202) 720-7373

Fax:
(202) 720-7708

E-Mail:
pdsd@usda.gov

Correcting Security Questionnaires: Use of FIPC 391 Form

Any changes made to an employee's/contractor's security questionnaire (SF86 or SF85P) must be initialed and dated by the Subject. Under certain limited circumstances, agencies may modify the form consistent with the Subject's intent.

Any changes made by agency officials must be initialed, dated, and identified by SOI or SON, for example "CM 10/1/04 AG00" next to each correction.

Agency officials must use an the **FIPC 391, Certification of Amended Investigative Form** to certify amended investigative forms were made consistent with the Subject's intent and made with the Subject's concurrence.

The personnel security official must first gain permission from the applicant/employee for any changes that are made.

Because we are not authorized to write on anyone's security questionnaire without permission, using the FIPC 391 to record ALL corrections/additions leaves us with a written record that we received such permission. This is especially important to have in those rare cases when employees claim they never authorized a reviewer to make such modifications to their forms.

Pop Quiz Answers!

1. 13
2. SBI
3. 3
4. E.O. 12958
5. E.O. 12968
6. Top Secret
7. 5
8. SCI
9. SCIF
10. SF-312

Final Thought…

If you would like to see PDSD address a particular topic, process, or guideline in a future newsletter, please submit your request to PDSD at pdsd@usda.gov.

We're on the Web!

See us at:

http://www.usda.gov/da/pdsd/